PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-249825
(43)Date of publication of application : 17.09.1999

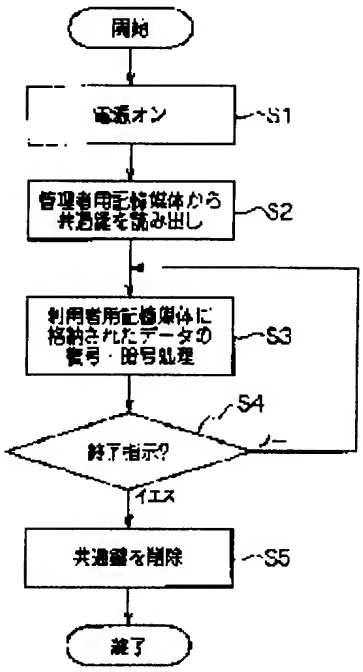
(51)Int.Cl. G06F 3/08
G09C 1/00
H04L 9/08

(21)Application number : 10-051889
(22)Date of filing : 04.03.1998

(71)Applicant : NEC CORP
(72)Inventor : FUJITA SHIGEKI

(54) COMMON KEY MANAGING METHOD, DATA READER USING THE SAME AND IC CARD SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To protect data from access from the third person to data in simple configuration.
SOLUTION: When the power source of a data reader for decoding and utilizing data stored in a storage medium for user is turned on (step S1), the mount of this storage medium for manager is requested to a manager and a common key is read out of the storage medium for manager (common key reading process, step S2). Further, the data stored in the storage medium for user are decoded while utilizing the common key read by this common key reading process (data decoding process, S3).



LEGAL STATUS

[Date of request for examination] 04.03.1998
[Date of sending the examiner's decision of rejection] 27.08.2002
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－249825

(43)公開日　平成11年(1999)９月17日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｇ０６Ｆ	3/08		Ｇ０６Ｆ	3/08	Ｃ
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ａ
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ａ

審査請求　有　　請求項の数９　ＯＬ　（全８頁）

(21)出願番号　　特願平10－51889

(22)出願日　　平成10年(1998)３月４日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　藤田　茂樹
東京都港区芝五丁目７番１号　日本電気株式会社内

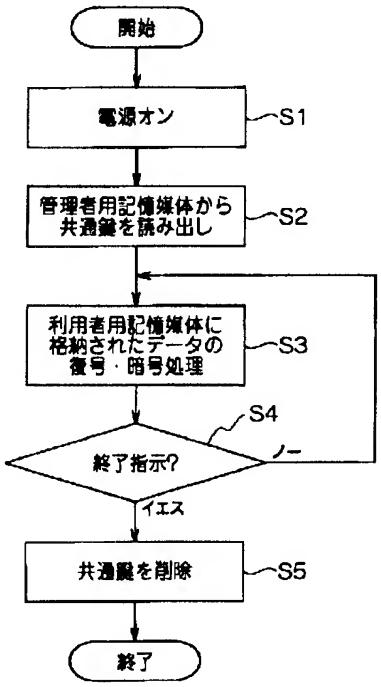
(74)代理人　弁理士　高橋　勇

(54)【発明の名称】　共通鍵管理方法およびこれを用いたデータ読み取り装置並びにＩＣカードシステム

(57)【要約】

【課題】　単純な構成でデータに対する第三者からのアクセスからデータを保護すること。

【解決手段】　利用者用記憶媒体３に格納されたデータを復号して利用するデータ読み取り装置２の電源がオンされると（ステップＳ１）、この管理者用記憶媒体１の装着を管理者に要求して、管理者用記憶媒体から共通鍵を読み出す（共通鍵読み出し工程，ステップＳ２）。さらに、この共通鍵読み出し工程によって読み出された共通鍵を使用して利用者用記憶媒体に格納されたデータを復号する（データ復号工程，Ｓ３）。



【特許請求の範囲】

【請求項１】　利用者のデータを格納する利用者用記憶媒体に格納されたデータを当該データの読み取り装置にて復号するための共通鍵を管理する方法であって、
前記利用者用記憶媒体に格納されたデータの暗号化に使用した共通鍵を当該共通鍵の管理者によって携帯される管理者用記憶媒体へ格納する共通鍵格納工程と、この共通鍵格納工程によって格納された共通鍵を読み出す共通鍵読み出し工程と、この共通鍵読み出し工程によって読み出された共通鍵を使用して前記利用者用記憶媒体に格納されたデータを復号するデータ復号工程とを備えたことを特徴とする共通鍵管理方法。

【請求項２】　前記共通鍵読み出し工程は、前記データの読み取り装置に電源が投入された時に実行されることを特徴とする請求項１記載の共通鍵管理方法。

【請求項３】　前記共通鍵読み出し工程が実行された後、前記データの読み取り装置の電源がオフされる指令を受けた時に当該読み取り装置内に読み出された共通鍵を削除する共通鍵削除工程を備えたことを特徴とする請求項１記載の共通鍵管理方法。

【請求項４】　利用者のデータを格納する利用者用記憶媒体に格納されたデータを当該データの読み取り装置にて復号するための共通鍵を管理する方法であって、
前記読み取り装置に電源が投入された時に前記共通鍵を管理する管理者によって携帯される管理者用記憶媒体から読み出す共通鍵格納工程と、前記利用者用記憶媒体にデータを格納する際に利用者別の鍵で当該データを暗号化する第１の暗号化工程と、この第１の暗号化工程で使用した利用者別の鍵を前記共通鍵を使用して暗号化する第２の暗号化工程と、前記第１の暗号化工程で暗号化されたデータと前記第２の暗号化工程で暗号化された利用者別の鍵とを前記利用者用記憶媒体に格納するデータ格納工程とを備えたことを特徴とする共通鍵管理方法。

【請求項５】　前記データ格納工程の後、データの読み取り装置によって読み出された前記共通鍵を当該読み取り装置内から削除する共通鍵削除工程を備えたことを特徴とする請求項４記載の共通鍵管理方法。

【請求項６】　利用者又は管理者によって携帯される記憶媒体が装着される装着部と、この装着部に装着された記憶媒体からデータを読み出すと共に当該記憶媒体へデータを書き込むリード／ライト部と、このリード／ライト部による読み出し動作および書き込み動作を制御する制御部と、この制御部に接続され一時的なデータを格納するメモリ部とを備えると共に、
前記制御部は、前記利用者によって携帯される記憶媒体には利用者別鍵によって暗号化したデータを格納すると共に共通鍵を使用して暗号化した利用者別鍵を格納させる利用者用格納手段と、前記管理者によって携帯される記憶媒体には前記共通鍵を格納させる管理者用格納手段とを備えたことを特徴とするデータ読み取り装置。

【請求項７】　前記制御部は、当該制御部の起動時に前記管理者用の記憶媒体の装着を要求する共通鍵要求手段と、この共通鍵要求手段による要求に応じて装着された管理者用の記憶媒体から共通鍵を読み出して前記メモリ部に保存する共通鍵保存手段と、前記利用者用記憶媒体が前記装着部に装着された時に当該メモリ部に格納された共通鍵を使用して復号する復号手段とを備えたことを特徴とする請求項６記載のデータ読み取り装置。

【請求項８】　前記制御部は、前記メモリ部に格納した共通鍵を当該制御部の動作終了制御時に消去する共通鍵消去手段を備えたことを特徴とする請求項７記載のデータ読み取り装置。

【請求項９】　データの利用者によって携帯される利用者用ＩＣカードと、データの管理者によって携帯される管理者用ＩＣカードと、この管理者用ＩＣカードおよび利用者用ＩＣカードに対してデータの記録又は再生を行うＩＣカードライタ装置とを備え、
前記利用者用ＩＣカードは、利用者別の鍵で暗号化されたデータと、この利用者別の鍵を共通鍵で暗号化したデータとを記憶する記憶領域を備え、
前記管理者用ＩＣカードは、前記共通鍵を記憶する記憶領域を備え、
前記ＩＣカードライタ装置は、前記管理者用ＩＣカードに格納された共通鍵を使用して前記利用者用ＩＣカードに格納された又は格納するデータの暗号化又は復号化を行う制御手段を備えたことを特徴とするＩＣカードシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、共通鍵管理方法に係り、特に、データ又は暗号化に使用する鍵を共通鍵で暗号化するシステムにて共通鍵を管理する管理方法に関する。本発明はさらに、このような方法を使用するのに適したデータ読み取り装置およびＩＣカードシステムに関する。

【０００２】

【従来の技術】記録媒体に格納したデータをアクセス権のない第三者から保護するためには、そのデータを暗号化するとよい。しかし、その暗号化に必要な鍵自体が盗まれてしまうと、第三者によりデータを復号されて、アクセスされてしまう。このため、１つの記憶媒体に暗号化したデータとこの暗号化で使用した鍵を格納する手法は、結局データの保護としては、必ずしも強固といえない場合が生じ得る。

【０００３】これに対して、鍵を二重化し、１つの鍵を別の記憶媒体に格納しておき、ユーザがそのデータを使用するときには２つの記憶媒体に格納された２つの鍵を使用してデータを復号する手法が提案されている。この場合、別の記憶媒体に格納しておく鍵は複数のユーザに対して共通のものでよい。このため、このような鍵の二

重化を行う手法を共通鍵方式という。

【０００４】

【発明が解決しようとする課題】この共通鍵方式では、複数の鍵を使用するため、共通鍵の提供の手法によってはシステム全体が複雑となってしう。しかし、データの保全（セキュリティ）が強固である限りにおいて、単純で安定して運用でき、かつ安価で実現することが望ましい。

【０００５】

【発明の目的】本発明は、単純な構成でデータに対する第三者からのアクセスからデータを保護することのできる共通鍵管理方法およびこれを用いたデータ読み取り装置並びにＩＣカードシステムを提供することを、その目的とする。

【０００６】

【課題を解決するための手段】そこで、本発明では、利用者のデータを格納する利用者用記憶媒体に格納されたデータを当該データの読み取り装置にて復号するための共通鍵を管理する方法であって、利用者用記憶媒体に格納されたデータの暗号化に使用した共通鍵を当該共通鍵の管理者によって携帯される管理者用記憶媒体へ格納する共通鍵格納工程と、この共通鍵格納工程によって格納された共通鍵を読み出す共通鍵読み出し工程と、この共通鍵読み出し工程によって読み出された共通鍵を使用して利用者用記憶媒体に格納されたデータを復号するデータ復号工程とを備えた、という構成を採っている。これにより前述した目的を達成しようとするものである。ここでは、共通鍵を管理者用の記憶媒体に格納する。そして、読み取り装置にて利用者用記憶媒体に格納されたデータの復号が必要となった場合には、この別途格納されていた管理者用記憶媒体中の共通鍵を使用する。このため、利用者用の記憶媒体のみが盗難され、解析されても、共通鍵は別途管理者用記憶媒体に格納されているため、利用者用のデータが盗まれることがない。このとき、共通鍵を管理者用の記憶媒体に格納したため、読み取り装置からネットワークを介して共通鍵を読み出す等の複雑な処理を必要とせず、ローカルな局面で安全に共通鍵を受け渡す。ここで、「記憶媒体」は、管理者が形態可能で共通鍵となるデータを記憶するものであればどのようなものでもよい。フロッピーディスクや、ＩＣカードや、またノート型パソコンのハードディスクなどを含む。共通鍵の変更を行わないのであれば、追記不能な光ディスクであってもよい。この方法の発明にあっては、管理者用の記憶媒体と利用者用の記憶媒体とは異なる媒体であっても良い。例えば、管理者用記憶媒体がＩＣカードであって、利用者用の記憶媒体は据えつけ型のコンピュータ内のハードディスクであってもよい。この場合、利用者用の記憶媒体とデータ読み取り装置とはネットワークで接続する。

【０００７】また、このような方法を使用するためのデータ読み取り装置として、本発明は、利用者又は管理者によって携帯される記憶媒体が装着される装着部と、この装着部に装着された記憶媒体からデータを読み出すと共に当該記憶媒体へデータを書き込むリード／ライト部と、このリード／ライト部による読み出し動作および書き込み動作を制御する制御部と、この制御部に接続され一時的なデータを格納するメモリ部とを備えている。しかも、制御部は、利用者によって携帯される記憶媒体には利用者別鍵によって暗号化したデータを格納すると共に共通鍵を使用して暗号化した利用者別鍵を格納させる利用者用格納手段と、管理者によって携帯される記憶媒体には共通鍵を格納させる管理者用格納手段とを備えた、という構成を採っている。ここでは、装着部が、管理者用の記憶媒体と利用者用の記憶媒体との両方を装着するため、共通鍵を管理者用の記憶媒体で管理するために特別な装置を別途設ける必要なく、ローカルに共通鍵の受け渡しを行う。このため、このデータ読み取り装置の発明にあっては利用者用記憶媒体と管理者用記憶媒体は同一の記録再生系でデータの記録および再生が可能な組み合わせとなる。例えば、双方をＩＣカードとするか、また、必要に応じて利用者用記憶媒体を光磁気ディスクとし、管理者用記憶媒体を光ディスクとするようにしてもよい。

【０００８】また、この読み取り装置の盗難に対しては、制御部は、メモリ部に格納した共通鍵を当該制御部の動作終了制御時に消去する共通鍵消去手段を備えると良い。すると、管理者が常駐しない場合には、読み取り装置内のメモリ部等には共通鍵が保存されていないため、当該読み取り装置および利用者用記憶媒体が同時に盗難されたとしても、データが復号化されることがない。

【０００９】

【発明の実施の形態】次に、本発明の実施の形態を図面を参照して説明する。本実施形態では、予め、利用者用記憶媒体３に格納されたデータの暗号化に使用した共通鍵は、当該共通鍵の管理者によって携帯される管理者用記憶媒体１へ格納されている（共通鍵格納工程）。そして、図１に示すように、利用者用記憶媒体３に格納されたデータを復号して利用するデータ読み取り装置２の電源がオンされると（ステップＳ１）、この管理者用記憶媒体１の装着を管理者に要求して、管理者用記憶媒体から共通鍵を読み出す（共通鍵読み出し工程，ステップＳ２）。さらに、この共通鍵読み出し工程によって読み出された共通鍵を使用して利用者用記憶媒体に格納されたデータを復号する（データ復号工程，Ｓ３）。このように、共通鍵を管理者用記憶媒体１に格納しておき、利用者のデータの復号を行う際に、又は、データ読み取り装置２の電源が投入されたときに共通鍵を管理者用記憶媒体から読み出すことで、ローカルな局面でネットワークを介せずに共通鍵を利用することができる。このため、

共通鍵を使用する店舗やフロア毎にそれぞれ個別に共通鍵方式によるデータのセキュリティの管理を行うことができる。

【００１０】また、図１に示す例では、共通鍵読み出し工程Ｓ２が実行された後、データの読み取り装置２の電源がオフされる指令（終了指令）を受けた時に（ステップＳ４）、当該読み取り装置内に読み出された共通鍵を削除する（共通鍵削除工程，Ｓ５）。この共通鍵削除工程を有すると、管理者が不在となる場合に読み取り装置の電源をオフとすることで、共通鍵は管理者が携帯する記憶媒体１以外には存在せず、従って、読み取り装置２や利用者用の記憶媒体３の内容を解析しても、データを復号することができず、これにより、データの管理を強固なものとすることができる。しかも、共通鍵をネットワーク上で管理する場合と比較して、構成が容易であり、システムが複雑とならず、これによっても、セキュリティを向上させることができる。

【００１１】図２は共通鍵を使用したデータの暗号化の手法を示すフローチャートである。暗号処理を開始するには、その前提として、管理者用の記憶媒体１から共通鍵を読み出さなければならない（ステップＳ１１）。これは、図１に示すように、読み取り装置２の電源投入時に行うようにしても良く、また、利用者用記憶媒体に記録されたデータを復号する必要が生じたときに管理者用の記憶媒体の装着を要求するようにしてもよい。

【００１２】共通鍵が読み出されると、まず、利用者別の鍵で当該データを暗号化する（第１の暗号化工程，Ｓ１１）。次いで、第１の暗号化工程Ｓ１１で使用した利用者別の鍵を共通鍵を使用して暗号化する（第２の暗号化工程，Ｓ１２）。さらに、第１の暗号化工程Ｓ１２で暗号化されたデータと第２の暗号化工程Ｓ１３で暗号化された利用者別の鍵とを利用者用記憶媒体に格納するデータ格納工程Ｓ１４とを備える。データ格納工程Ｓ１４では、利用者別の鍵を共通鍵で暗号化する処理を待ってから当該暗号化したデータを格納する処理を図示したが、データ格納工程Ｓ１４は、ステップＳ１２にてデータの暗号化が行われた場合にはステップＳ１３とＳ１４とを並行して処理する場合を含む。

【００１３】また、この暗号化が終了する度に、すなわち、データ格納工程Ｓ１４の後、データの読み取り装置によって読み出された共通鍵を当該読み取り装置内から削除する共通鍵削除工程を備えるようにしても良い。これにより、データ読み取り装置は共通鍵を最低限必要な場合にのみ保持する。

【００１４】図３はデータ読み取り装置の構成を示すブロック図である。図３に示すように、データ読み取り装置は、利用者又は管理者によって携帯される記憶媒体１，３が装着される装着部１０と、この装着部１０に装着された記憶媒体からデータを読み出すと共に当該記憶媒体へデータを書き込むリード／ライト部１２と、このリード／ライト部１２による読み出し動作および書き込み動作を制御する制御部１４と、この制御部１４に接続され一時的なデータを格納するメモリ部とを備えている。

【００１５】しかも、制御部１４は、利用者によって携帯される記憶媒体３には利用者別鍵によって暗号化したデータを格納すると共に、共通鍵を使用して暗号化した利用者別鍵を格納させる利用者用格納手段１８と、管理者によって携帯される記憶媒体には共通鍵を格納させる管理者用格納手段１９とを備える。この制御部１４は、プログラムを逐次実行することでデータの処理およびリード／ライト部１２の制御を行うプロセッサを備える。また、プロセッサに代えて、所定の機能を実現するための論理回路としてもよい。

【００１６】制御部１４がプロセッサを有する場合には、制御部１４の各手段はプログラムにより実現する。この場合、メモリ部１６又は制御部１４ないに有する例えばＲＯＭに、プロセッサを利用者用格納手段として動作させるプログラムと、プロセッサを管理者用格納手段１９として動作させるプログラムとを格納する。制御部１４のその他の機能についても同様である。

【００１７】さて、好ましくは、制御部１４は、当該制御部１４の起動時に管理者用の記憶媒体の装着を要求する共通鍵要求手段と、この共通鍵要求手段による要求に応じて装着された管理者用の記憶媒体から共通鍵を読み出してメモリ部に保存する共通鍵保存手段と、利用者用記憶媒体が装着部に装着された時に当該メモリ部に格納された共通鍵を使用して復号する復号手段とを備えるとよい。これらの手段により、図１又は図２に示した各工程を実現することができる。制御部１４はさらに、メモリ部に格納した共通鍵を当該制御部の動作終了制御時に消去する共通鍵消去手段を備えるとよい。

【００１８】図３に示す装着部は、管理者用の記憶媒体又は利用者用の記憶媒体の双方を装着できるものが望ましい。すると、１台のデータ読み取り装置、例えば、記憶媒体がＩＣカードである場合には、ＩＣカードライタにより図１および図２に示す共通鍵管理方法を実現することができる。従って、共通鍵を管理するための装置をより単純で簡易なものとすることができる。また、記憶媒体をフロッピーディスクとする場合には装着部１０をフロッピーディスクドライブとするなど、装着部の構成については適宜必要に応じて設計変更を行う。

【００１９】次に、ＩＣカードシステムの実施形態を説明する。図４に示す例では、ＩＣカードシステムは、データの利用者によって携帯される利用者用ＩＣカード３と、データの管理者によって携帯される管理者用ＩＣカード１と、この管理者用ＩＣカードおよび利用者用ＩＣカードに対してデータの記録又は再生を行うＩＣカードライタ装置３とを備えている。このＩＣカードライタ装置３としては、例えば図３に示したデータ読み取り装置

を使用する。

【００２０】そして、利用者用ＩＣカード２は、利用者別の鍵K1で暗号化されたデータ（$E_{(K1)}DN$）と、この利用者別の鍵K1を共通鍵で暗号化したデータ（$E_{(K2)}K1$）とを記憶する記憶領域（図中格子の部分）を備えている。また、管理者用ＩＣカードは、共通鍵K2を記憶する記憶領域を備えている。そして、ＩＣカードライタ装置は、管理者用ＩＣに格納された共通鍵を使用して利用者用ＩＣカードに格納された又は格納するデータの暗号化又は復号化を行う制御手段（図示せず）を備える。

【００２１】ここでは、データを暗号化する利用者別の鍵K1が存在し、そのK1を共通鍵K2により暗号化し、利用者が利用するＩＣカードに（$E_{(K2)}K1$）として格納する。また、管理者用のＩＣカード１内に共通鍵鍵K2を格納する。そして、利用者の使用するデータＤＮは利用者ＩＣカードにK1にて暗号化し、利用者ＩＣカードに（$E_{(K1)}DN$）として格納する。

【００２２】まず、装置３を起動する際に、管理者用ＩＣカードを要求する。その時に管理者本人を確認する必要があるため、ＩＣカードにあらかじめ格納されているパスワード（暗証番号）で本人を確認するようにしてもよい。また、そのパスワードの照合によって、管理者用ＩＣカードのK2にアクセスできる権限を与える。すると、管理者用のカードが盗難された場合であっても、利用者のデータが保護される。また、その認証がうまく行かない場合、装置３を起動させなくし、またアプリケーションの利用を拒否するなどの処理を適宜実施すると良い。

【００２３】パスワードの照合が成功すると、管理者用のＩＣカードから利用者別鍵K1を復号化するための共通鍵K2を読み出し、共通鍵K2を装置内部のメモリ部１６（ＲＡＭまたはＨＤＤ上）に格納する（ステップ１ａ）。そして、利用者が装置を使用する際に、利用者のＩＣカードから（$E_{(K2)}K1$）を読み出し（ステップ２ｂ）、装置内部にて共通鍵K2により復号化し（ステップ３ｆ）、利用者別の鍵K1を生成させる。この利用者別の鍵K1により、ＩＣカード２内のデータ及び装置３内のデータが暗号・復号化する。例えば、暗号化されたデータ（$E_{(K1)}DN$）を読み出し、装置３の内部にてK1により復号化し（ステップ３ｉ）、データDNとして使用可能となる。

【００２４】また、装置内部に格納されている暗号化データ（$E_{(K1)}D2$）を使用する際も、K1を使用して復号化できる。さらに、利用者及び装置内部にて生成されたデータD3もK1を利用し、暗号化し、（$E_{(K1)}D3$）としＩＣカード２に格納できる。そして、利用者が使用を終了し、ＩＣカードを抜くときには、装置内にあるK1及び（$E_{(K2)}K1$）は抹消する。また、装置電源断時に、共通鍵K2も装置上（メモリ部上又はＨＤＤ等）から抹消される。

【００２５】これにより、ネットワークを介してK2及びK1を取得する必要がなく、K2を取得する際にも、ＩＣカードリーダライタも利用者が使用できるものと共有できる。また、利用者はＩＣカード内にK2及び生のK1（暗号化されていないK1）を持つ必要がないため、ＩＣカードが盗難等にあった場合でもＩＣカード内の暗号化されたデータを復元されることはない。また、利用者の利用終了及び装置電源断時にはK1、K2（$E_{(K2)}K1$）は装置内から抹消されるため、装置から暗号化されたデータを盗まれてもデータを復元されることはない。

【００２６】また、場合によっては（$E_{(K2)}K1$）は、必要時のみ読み込むことも可能である。すなわち、読み込んでは消去し、読み込んでは消去するなど、アプリケーションの作成手法次第となる。

【００２７】上述したように本実施形態によると、利用者用ＩＣカードにデータを暗号・復号鍵を暗号化したデータを入れ、管理者用のＩＣカードへ鍵を復号化する鍵を入れ、そのＩＣカードより、電源投入時に鍵を装置内に読み込み、電源断時にその鍵を装置内から抹消するため、ネットワークを使用せずに共通鍵を利用することができる。すると、共通鍵の利用をローカルな場所にて安定してかつ高速に行うことができ、さらには何らかの問題によりネットワークがストップした場合、鍵を取得できなくなり、暗号、復号化ができなくなることがない。

【００２８】ネットワークを介して鍵を取得することは、ネットワークへのアクセス時間及びネットワーク構築によるシステムの複雑化につながる。利用者ＩＣカードへの鍵の格納及び装置内への鍵の格納は、データ解読の可能性があり危険であり、また装置内に鍵を持ちつづけることは管理者不在時（電源ＯＦＦ時）に何らかの方法で装置にアクセスされ、鍵を盗まれる可能性がある。これを防ぐために、管理者用ＩＣカードを準備し、そのＩＣカードへ鍵を暗号化した鍵を書き込み、電源投入時に鍵を暗号化した鍵を装置内に読み込み、利用者がＩＣカードを挿入した際にデータを暗号・復号化する鍵（管理者用ＩＣカードの鍵によって暗号化された鍵）を読み込み、装置内で復号化し、データの暗号・復号に利用する。

【００２９】電源ＯＦＦ時には管理者用ＩＣから読み込んだ鍵を抹消する（当然利用者ＩＣカードから読み込んだ暗号化された鍵は、ＩＣカードを抜いた際に抹消されている）。この時、管理者が利用するＩＣカードリーダライタは利用者が利用するものと同じ物が使用可能なため、ＩＣリーダライタは１個あればよい。

【００３０】さらに、図３に示す例では、ＩＣカードリードライタを２つ設置し、暗号鍵取得ＩＣカード専用のリーダライタを設ける方式を採る必要がなくなり、すると、ＩＣカードリーダライタを複数個設置することにより、装置単価が上がるという不都合が生じない。

【００３１】さらに、利用者別の鍵を共通鍵で暗号化し

てから利用者のＩＣカード内に両方とも格納するため、ＩＣカード利用者またはＩＣカードを取得した人がＩＣカード内のデータを読み取ることにより、無差別にデータ及び暗号鍵を解読することにより、暗号化データが解読されてしまうことがない。

【００３２】そして、装置の電源がオフとなった時には装置内から共通鍵を削除する構成を採用することで、何らかの方式で装置に直接アクセスし、鍵が盗まれ、データが解読される可能性がなくなる。

【００３３】

【実施例】上記実施の形態で述べた形態にて、一般の人が使用できるＫＩＯＳＫ端末等にＩＣカードリーダライタを内蔵し、同様のことを実施することが可能である。例えば、ある店舗にＫＩＯＳＫ端末を設置し、毎朝店の責任者が管理者カードを使用し、端末を起動させる。そこで、ＫＩＯＳＫ端末の会員等にＩＣカードを利用し、ＫＩＯＳＫ端末を利用して頂く。

【００３４】その場合、会員のみが見ることができるデータ等を暗号化して装置の中に入れておき、ＩＣカードの認証とともに、データが取り出せる（又は見られるようにする）。この時、その端末のみで実施しようとした場合、鍵はネットワーク等により外部から取得する必要がないため、ローカルにて暗号・復号化が可能となる。

【００３５】このように本実施例によると、鍵を管理者用ＩＣカードに格納することにより、ネットワークを介して鍵を取得する必要がないため、暗号・復号による時間のロスが少ない、またネットワークを構築する必要がなく、システムが簡略化され、ローカルにて暗号、復号が可能である。

【００３６】鍵を暗号化して利用者ＩＣカードに格納し、管理者用のＩＣカードに鍵を復号化する鍵を格納することにより、ＩＣカード利用者自身及び管理者が直接鍵を管理しているわけではないため、ＩＣカード利用者及び管理者はＩＣカード内に格納されているデータを解読されることはない。

【００３７】鍵を暗号化して利用者ＩＣカードに格納し、管理者用のＩＣカードに鍵を復号化する鍵を格納することにより、装置内にあるその鍵で暗号化されたデータはデータそのものを盗まれたとしてもそのデータは解読されることはない。

【００３８】また、管理者用カード、利用者用カードが盗難にあっても、二つともそろわない限り、データを解読されることはない。

【００３９】鍵を暗号化して利用者ＩＣカードに格納し、管理者用のＩＣカードに鍵を復号化する鍵を格納することにより、装置起動時に利用者が利用するＩＣカードリーダライタから鍵を復号する鍵を装置内に読み込むため、他のＩＣカードリーダライタを使用し、そのＩＣカードから鍵を読み込む必要がなく、ＩＣカードリーダライタは利用者用ＩＣカードリーダライタと共有できるため、専用のＩＣカードリーダライタを設ける必要がない。

【００４０】また、利用者別の鍵K1を共通鍵K2により暗号化し、その（E(K2)K1）及びK2は別々のカードに保存されるため、暗号化、復号化の鍵K1を装置、利用者ＩＣカード、管理者ＩＣカードに、生のまま存在しないため、何らかのカードが盗まれた場合でも、暗号化されたデータは復号することはできない。そして、電源ＯＦＦ時に共通鍵を消滅させるため、電源が切れているときは鍵を装置が持っておらず、これにより、深夜など、管理者がいないときにデータが盗まれても、そのデータの中身を見ることができない。

【００４１】

【発明の効果】本発明は以上のように構成され機能するので、これによると、読み取り装置にて利用者用記憶媒体に格納されたデータの復号が必要となった場合には、別途格納されていた管理者用記憶媒体中の共通鍵を使用するため、利用者用の記憶媒体のみが盗難され、解析されても、利用者用のデータが盗まれることがなく、そして、共通鍵を管理者用の記憶媒体に格納したため、読み取り装置からネットワークを介して共通鍵を読み出す等の複雑な処理を必要とせず、ローカルな局面で安全に共通鍵を受け渡すことができ、これにより、単純な構成で信頼性の高いデータの管理を実現できるという従来にない優れた共通鍵管理方法を提供することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態による共通鍵の管理方法の処理工程を示すフローチャートである。

【図２】図１に示した共通鍵を使用してデータを暗号化する処理例を示すフローチャートである。

【図３】本実施形態によるデータ読み取り装置の構成を示すブロック図である。

【図４】本実施形態によるＩＣカードシステムでののデータ、及び鍵の流れを示す説明図である。

【符号の説明】

K1　データを暗号・復号化する鍵

K2　K1を暗号・復号化する鍵

パスワード　管理者を認識するパスワード

E(K*)（**）　データ＊＊を鍵Ｋ＊で暗号化したデータ

Ｄ(K*)（E(K*)（**））　データ（E(K*)（**））を鍵Ｋ＊で復号化するデータ**

１　管理者用記憶媒体（例えば、ＩＣカード）

２　利用者用記憶媒体（例えば、ＩＣカード）

３　データ読み取り装置（例えば、ＩＣカードライタ装置）

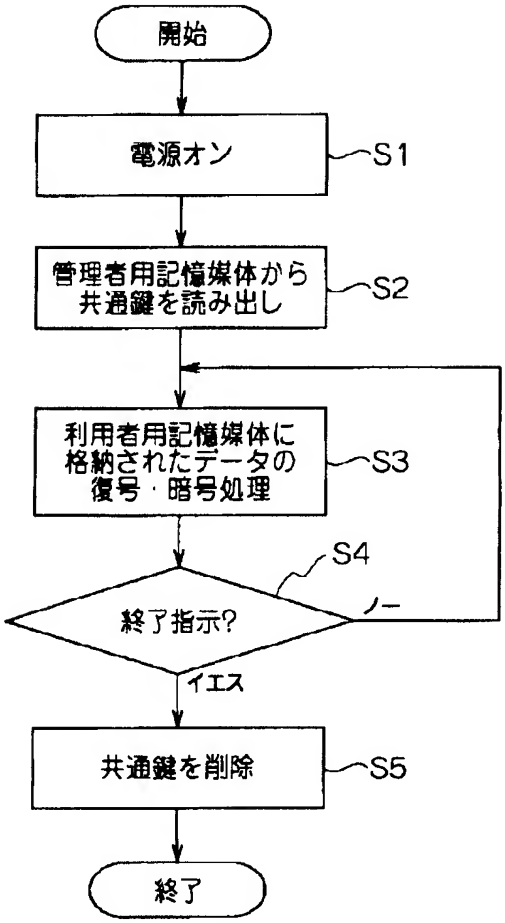
１０　装着部

１２　リード／ライト部

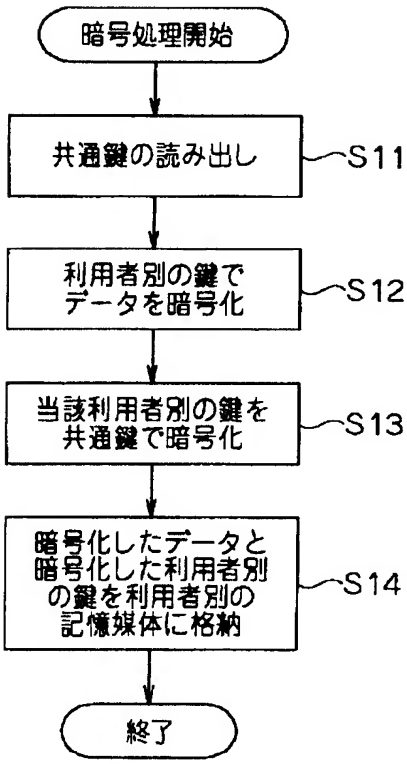
１４　制御部

１６　メモリ部（ＨＤＤやＲＡＭ等）

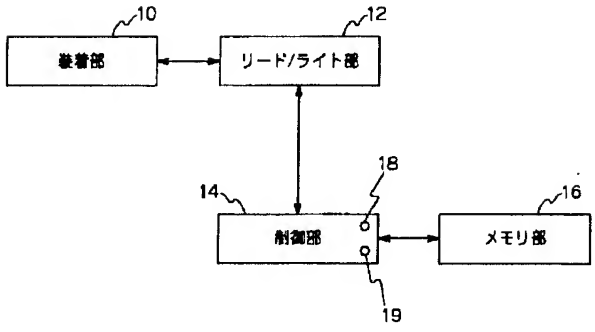
【図１】


開始
電源オン
S1
管理者用記憶媒体から
共通鍵を読み出し
S2
利用者用記憶媒体に
格納されたデータの
復号・暗号処理
S3
S4
終了指示?
ノー
イエス
共通鍵を削除
S5
終了

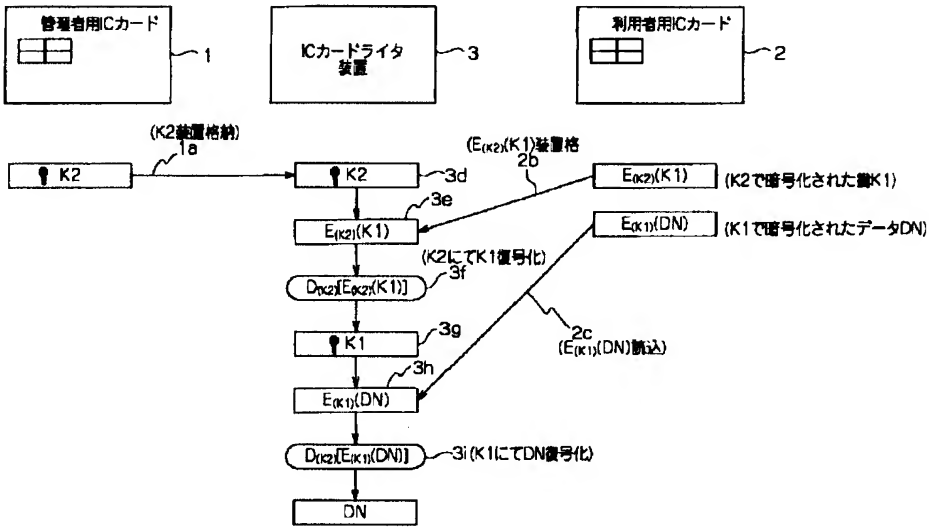
【図２】


暗号処理開始
共通鍵の読み出し
S11
利用者別の鍵で
データを暗号化
S12
当該利用者別の鍵を
共通鍵で暗号化
S13
暗号化したデータと
暗号化した利用者別
の鍵を利用者別の
記憶媒体に格納
S14
終了

【図３】


10
12
装着部
リード/ライト部
14
18
16
制御部
メモリ部
19

【図４】


管理者用ICカード
1
ICカードライタ装置
3
利用者用ICカード
2
(K2装置格納)
1a
K2
K2
3d
(E(K2)(K1)装置格納)
2b
E(K2)(K1)
(K2で暗号化された鍵K1)
3e
E(K2)(K1)
E(K1)(DN)
(K1で暗号化されたデータDN)
(K2にてK1復号化)
3f
D(K2)[E(K2)(K1)]
K1
3g
2c
(E(K1)(DN)読込)
3h
E(K1)(DN)
D(K2)[E(K1)(DN)]
3i(K1にてDN復号化)
DN